The Florida House of Representatives

Interim Project Report January 2006

Governmental Operations Committee Representative David Rivera, Chair

Personal Information Protection Act
A White Paper

PURPOSE

Since its inception, Florida's public records law has undergone significant changes. These changes resulted from the state's growing technological capabilities coupled with its desire to have the most open government records policy in the nation, while at the same time protecting, through exemptions, information that, if disclosed, could cause harm. However, what began as a desire to place our government "in the sunshine," and to provide citizens with the right to inspect public records, has resulted in the dissemination of a tremendous amount of personal information through electronic means. The ever-increasing volume of information collected by governmental agencies has created tension between the state's public records law and the right to privacy.

In an attempt to address these issues, the Speaker of the House of Representatives approved an interim project by the Governmental Operations Committee regarding protecting and restricting access to social security numbers held by Florida government. The purpose of the project was to explore and research measures to protect personal information in the custody of Florida government.

BACKGROUND

PUBLIC RECORDS LAW

CONSTITUTION

Article I, s. 24(a), Florida Constitution, sets forth the state's public policy regarding access to government records. The section guarantees every person a right to inspect or copy any public record of the legislative, executive, and judicial branches of government. The Legislature may, however, provide by general law for the exemption of records from the requirements of Article I, s. 24(a), Florida Constitution. The general law must state with specificity the public necessity justifying the exemption (public necessity statement) and must be no broader than necessary to accomplish its purpose.

FLORIDA STATUTES

Public policy regarding access to government records also is addressed in the Florida Statutes. The Public Records Act[1] guarantees every person a right to inspect and copy any state, county, or municipal record.[2] Furthermore, the Open Government Sunset Review Act[3] provides that a public records exemption may be

[1] Chapter 119, F.S.
[2] Section 119.07(1), F.S.
[3] Section 119.15, F.S.

created or maintained only if it serves an identifiable public purpose, and may be no broader than necessary to meet one of the following public purposes:

- Allows the state or its political subdivisions to effectively and efficiently administer a governmental program, which administration would be significantly impaired without the exemption;
- Protects sensitive personal information that, if released, would be defamatory or would jeopardize an individual's safety. However, only the identity of an individual may be exempted under this provision; or,
- Protects trade or business secrets.

RIGHT TO PRIVACY

Article I, section 23, Florida Constitution, provides "every natural person" with the right to be let alone and free from government intrusion into that person's private life. The right to privacy cannot be construed to limit the public's right of access to public records and meetings.

The relationship between the right to access public records and the right to privacy has been addressed by Florida courts. In *Board of Country Commissioners of Palm Beach County v. D.B.*, the Fourth District Court of Appeal held: "[I]n Florida the right to privacy is expressly subservient to the Public Records Act . . . Florida's right to privacy provision states that the right to privacy 'shall not be construed to limit the public's right of access to public records.'"[4]

In *Dean Forsberg & Walter Freeman v. The Housing Authority of the City of Miami Beach & Murray Gilman*, the Florida Supreme Court noted that public records are open for personal inspection, which included the records of the housing authority. The court further stated: "This case, therefore, deals solely with access to public records. While certain records are statutorily exempted from the public's right to inspect, our examination of the statutes has brought to light no exemption pertaining to the records involved in this appeal . . . There is, likewise, no state constitutional right to privacy which would shield these records . . . Moreover, adoption of the privacy amendment offers no relief in this case because section 23 specifically does not apply to public records."[5]

Therefore, unless the Legislature specifically exempts information from public disclosure in the Florida Statutes, the constitutional right to access public records supersedes the constitutional right to privacy.

2001 INTERIM PROJECT

During the 2001 interim, the former House Committees on State Administration and Information Technology surveyed agencies regarding government's collection, use, and

---

[4] *Board of County Commissioners of Palm Beach County v. D B.*, 784 So. 2d 585, 591 (Fla. 4th DCA 2001). Similarly, in *Wallace v. Guzman* [687 So. 2d 1351, 1354 (Fla. 3d DCA 1997)], the Third District Court of Appeal ruled: "[Patricia B. Wallace] urges that we balance her federal privacy right against the public's right to know. We conclude, however, that the people of our state and our legislature have already balanced such interests. The people have spoken through Article 1, section 23, Florida Constitution, which provides: 'Right of Privacy. Every natural person has the right to be let alone and free from governmental intrusion into his private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.'"

[5] 455 So. 2d 373, 374 (Fla. 1984) (citations omitted).

disclosure of social security numbers (SSN). The SSN was selected because it is the only nationwide, unique numeric form of identification, and it is often the link to an individual's personal records. As a result of the survey, the committees discovered that many agencies did not have a specific statutory exemption prohibiting the release of SSNs pursuant to a public records request.

As a result, the 2002 legislature passed a general public records exemption for SSNs held by an agency.[6]

PUBLIC RECORDS EXEMPTIONS FOR SOCIAL SECURITY NUMBERS

Currently, 121 sections of the Florida Statutes require collection of SSNs, and 32 of those sections provide specific public records exemptions for such numbers. The Florida Statutes contain approximately 70 public records exemptions for SSNs; 54 specifically for such number and 16 for personal identifying information, which includes the SSN.

In 2002, the legislature passed a general exemption for social security numbers held by an agency.[7] Such number is made confidential and exempt from public disclosure;[8] however, an agency may release the SSN to another governmental entity in the furtherance of its duties and responsibilities.[9]

An agency also may release such number to a commercial entity "engaged in the performance of a commercial activity" provided the SSNs are "used only in the normal course of business for legitimate business purposes."[10] The commercial entity is required to make a verified written request[11] that is legibly signed in order to receive access to SSNs.

The exemption prohibits agencies from collecting SSNs unless authorized by law to do so or unless collection is otherwise imperative for an agency to perform its duties and responsibilities.[12] It also requires agencies to:

- Segregate such number on a separate page from the rest of the record in order to make redaction[13] of SSNs easier.[14]
- Provide a statement of the purpose or purposes for collecting SSNs.[15]

---

[6] Chapter 2002-256, L.O.F., s. 119.071(5)(a), F.S.

[7] *Id.*

[8] This exemption does not apply to the clerks of court. A person, however, who finds his or her SSN on a clerk website, is authorized to provide a written request to the clerk requesting that his or her SSN be removed from the website. The clerk must comply with the request at no charge. Beginning January 1, 2007, the clerks are required to actively protect the release of SSNs without receipt of a written request. Section 119.071(5)(a)7.g., F.S.

[9] Section 119.071(5)(a)4., F.S.

[10] Section 119.071(5)(a)5., F.S.

[11] The request must be verified as provided in s. 92.525, F.S. The section provides that a request is verified if made under oath or affirmation taken or administered before an officer authorized to administer oaths, or by signing a written declaration. The verified written request must include the name of the business, business mailing and location addresses, business telephone number, statement of specific purposes for needing access to SSNs, and how SSNs will be used in the normal course of business. Section 119.071(5)(a)5., F.S.

[12] Section 119.071(5)(a)2., F.S.

[13] "Redact" means to conceal from a copy of an original public record, or to conceal from an electronic image that is available for public viewing, that portion of the record that contains confidential or exempt information. Section 119.011(12), F.S.

[14] *Id.*

[15] *Id.*

- File a report each January 31 that provides the name of each business requesting access to SSNs and the reasons stated as the need for access.[16]

Finally, penalty provisions are provided for violating the exemption,[17] and a person is given the option to petition the court for compliance with the exemption.[18]

RECENT EVENTS

In the past couple of years, the databases of two national data brokers were compromised. ChoicePoint's database placed 145,000 consumers nationwide, 10,000 of which were Floridians, at risk for identity theft as a result of the data theft. ChoicePoint is the largest data collection business in the country. The company maintains and sells background files on virtually every adult American, compiled from millions of public and private records.[19] The database was compromised when criminals set up fake companies and downloaded information from ChoicePoint. The criminals posed as legitimate businesses in order to gain access to the various ChoicePoint databases. The databases contain consumer data, including names, addresses, SSNs, and credit reports.[20]

The LexisNexis Group also reported a breach that affected 320,000 consumers.[21] LexisNexis said access might have been gained by unauthorized use of passwords of legitimate subscribers to its databases. The breach involved databases acquired in July 2004, through a $775 million purchase of Seisint, a company based in Florida that compiled consumer background and asset information.[22]

FINDINGS

OTHER STATES – PROTECTION OF SOCIAL SECURITY NUMBERS

The following are a few examples of laws in other states governing access to SSNs:

- Georgia law prohibits general public access to SSNs; however, the media can obtain access if a written request is submitted under oath confirming that the media representative needs the number in connection with news gathering and reporting.
- Michigan exempts records that disclose an individual's SSN.
- Missouri exempts SSNs from public disclosure, unless disclosure is permitted by federal law, federal regulation, or state law; unless disclosure is authorized by the holder; or unless disclosure is for use in a civil, criminal, administrative, or arbitration proceeding.

[16] Section 119.071(5)(a)8., F.S.
[17] Section 119.071(5)(a)6., F.S.
[18] Section 119.071(5)(a)9., F.S.
[19] In 2004, ChoicePoint paid the Department of Highway Safety and Motor Vehicles more than $13.7 million for driver records. "ChoicePoint says it bought records of 10,000 Floridians" by Dara Kam, *The Palm Beach Post*, February 25, 2005.
[20] "Data theft affects 145,000 nationwide; ChoicePoint says it will notify all potential victims" by Bob Sullivan, MSNBC, February 16, 2005, at 10:37 p.m.
[21] "LexisNexis acknowledges more ID theft" by Caleb Silver, *CNN Business News*, June 2, 2005.
[22] "Another Data Broker Reports a Breach" by Tom Zeller, Jr., *The New York Times*, March 10, 2005.

- Tennessee prohibits a state entity from publicly disclosing a person's SSN.[23]

OTHER STATES – PERSONAL INFORMATION PROTECTION ACT

The following states have public records laws, and are recognizing the increased role of technology in the application and interpretation of such laws.

CALIFORNIA

In 1977, California recognized the increased role of technology and its effect on a citizen's privacy. As a result, California enacted the Information Practices Act. The act recognizes the fundamental right to privacy enumerated by both the California Constitution and the United States Constitution. The California legislature based this legislation on the following findings:

- The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies;
- The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information; and
- In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.[24]

California also recognized the role that state agencies play in the collection and dissemination of personal information. The Information Practices Act states: "Each agency shall maintain in its records only personal information which is relevant and necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the Federal Constitution."[25]

The law also requires each state department and state agency to enact and maintain a permanent privacy policy that adheres to the Information Practices Act of 1977. The privacy policy must address the following principles:

- Personally identifiable information is only obtained through lawful means;
- The purposes for which personally identifiable data are collected are specified at or prior to the time of collection, and any subsequent use is limited to the fulfillment of purposes not inconsistent with those purposes previously specified;
- Personal data shall not be disclosed, made available, or otherwise used for purposes other than those specified, except with the consent of the subject of the data, or as authorized by law or regulation;
- Personal data collected must be relevant to the purpose for which it is collected; and
- The general means by which personal data is protected against loss, unauthorized access, use modification or disclosure shall be posted, unless such disclosure of general means would compromise legitimate state department or state

[23] Fax entitled "Social Security Numbers," The National Conference of State Legislatures, November 15, 2004.

[24] California Codes, Civil Code, section 1798.1.

[25] California Codes, Civil Code, section 1798.14.

agency objectives or law enforcement purposes.[26]

Further, each state department or agency must designate a position within the department or agency with the responsibility of maintaining the privacy policy.[27]

California has an Office of Privacy Protection within the Department of Consumer Affairs. The office's purpose is to protect the privacy of individuals' personal information in a manner consistent with the California Constitution. This is accomplished by identifying consumer problems in the privacy area and facilitating development of fair information practices in adherence with the Information Practices Act of 1977.[28]

NEW YORK

New York's "Personal Privacy Protection Law" addresses state agency responsibilities when collecting personal information. The law requires that each agency that maintains a system of records to, "[e]xcept when a data subject provides an agency with unsolicited personal information, maintain in its records only such personal information that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order, or to implement a program specifically authorized by law."[29]

No agency may disclose any personal information unless such disclosure is pursuant to a written request by or the voluntary written consent of the data subject, provided that such request or consent by its terms limits and specifically describes:

- The personal information for which disclosure is requested;
- The person or entity to whom such personal information is requested to be disclosed; and
- The uses which will be made of such personal information by the person or entity receiving it.[30]

Finally, "personal information" is defined in New York's Personal Privacy Protection Law as "any information concerning a data subject which, because of name, number, symbol, mark or other identifier, can be used to identify that data subject."[31] This definition clearly includes an identifier such as a social security number.

TEXAS

Texas law relating to state government privacy policies, states that an individual has the right to be informed about information that is collected. More specifically: "It is the policy of this state that an individual is entitled to be informed about information that a state governmental body collects about the individual unless the state governmental body is allowed to withhold the information."[32]

The law acknowledges the right of an individual to receive notice about certain information laws and practices: "Each state governmental body that collects information about an individual by means of an Internet site or that collects information about the computer network location or identity of a

[26] California Government Code, section 11019.9.
[27] *Id.*
[28] Section 1, Article 7 to Chapter 4 of Division 1 of the Business and Professions Code.
[29] New York State Consolidated Laws, Article 6-A, section 94(a), Personal Privacy Protection Law.
[30] *Id.* at section 96(a).
[31] *Id.* at section 92(7).
[32] HB 1922, Title 5, Chapter 559, Texas Government Code, 2001.

user of the Internet site shall prominently post on the Internet site what information is being collected through the site about the individual or about the computer network location or identity of a user of the site, including what information is being collected by means that are not obvious."[33]

State agencies must be very specific about the information that is collected, and must inform citizens about any information that will be gathered without their knowledge.

VIRGINIA

Virginia law acknowledges the importance of personal privacy in the age of technology. In the "Government Data Collection and Dissemination Practices Act," the Virginia General Assembly found that

- An individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;
- The increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;
- An individual's opportunities to secure employment, insurance, credit, and [that individual's] right to due process, and other legal protections are endangered by the misuse of personal information systems; and
- In order to preserve the rights guaranteed a citizen in a free society, legislation is necessary to establish procedures to govern information systems containing records on individuals.[34]

Based on these findings, the Virginia General Assembly established several principles to ensure safeguards for personal privacy:

- Information shall not be collected unless the need for it has been early established in advance;
- There shall be a clearly prescribed and uncomplicated procedure for an individual to learn the purpose for which information has been recorded and the particulars about its use and dissemination;
- There shall be a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information;
- There shall be a clearly prescribed procedure to prevent personal information collected for one purpose from being used for another purpose; and
- The Commonwealth or any agency or political subdivision thereof shall not collect personal information except as explicitly or implicitly authorized by law.[35]

CONCLUSION

Florida's public records law has undergone tremendous change since its inception in 1909. Enhanced technological capabilities have expedited both the retrieval and dissemination of information. While most

[33] Section 1. Subtitle A, Title 5, Government Code, Chapter 559.

[34] Section 2.2-3800(B), Effective October 1, 2001, Short title; findings; principles of information practice.

[35] Section 2.2-3800(C), Effective October 1, 2001, Short title; findings; principles of information practices.

would agree that new technology has improved the delivery of both public and private services, and made information more accessible to the public, it is difficult to ignore the corresponding problems that have arisen. Namely, the abundance of personal information that is being collected from individuals, and the disclosure of such information through the Internet or other forms of electronic transmission. Personal information is becoming more easily and readily available; a click of the mouse can retrieve documents containing an individual's social security number, divorce record, financial information, and other sensitive information.

The State of Florida has the most open government records law in the nation. However, the increasing collection of personal information coupled with the growth in technology is making it increasingly difficult to preserve both a citizen's right to privacy and security and an effective open records law. This white paper has highlighted the numerous issues that are involved in the increased collection and dissemination of personal information. Many different entities are involved, and there are no obvious solutions. However, because technological growth has no boundaries, it is important that steps be taken to find the appropriate balance between open records and the protection of citizens' personal information.